Ref.4

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059354
(43)Date of publication of application : 25.02.2000

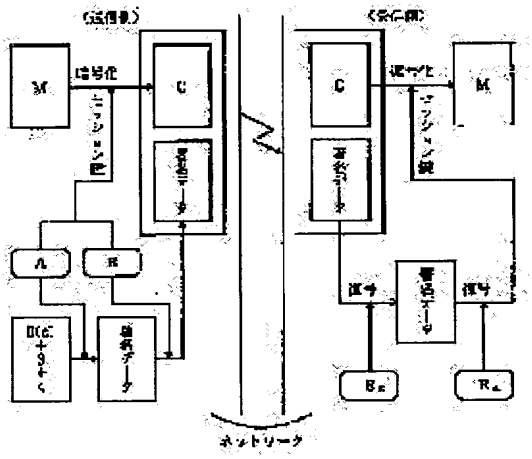
(51)Int.Cl. H04L 9/10
G09C 1/00
H04L 9/08

(21)Application number : 10-224433
(22)Date of filing : 07.08.1998

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : YANO YOSHIHIRO
HAYASHI MASAHIRO
HANDA TOMIO
HIRANO TANITAKE

(54) METHOD FOR GENERATING SESSION KEY WHILE UTILIZING PORTABLE RECORDING MEDIUM AND DATA DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To avoid the danger of having a key decoded by storing key tables for generating the public keys and the session keys of parties mutually on the sides of transmission and reception, and letting flow only the combination data of indexes of generating the keys for session to a network.
SOLUTION: Corresponding to the session key obtained by combining indexes generated at random from portable recording media A and B, transmission information M is enciphered so that a code sentence C is prepared. On the other hand, a hash value Hc obtained by performing hash processing to the code sentence C and the combined information of indexes 3 and 4 generated at random are respectively digitally signed by using the secret keys of the portable recording media A and B and transmitted onto the network together with the code sentence C. On the side of reception, the table indexes 3 and 4 are decoded by public keys EA and EB of the held recording media A and B, and the session key is acquired from the same key table stored on the reception side. Then the code sentence C is decoded by this key so that the transmission information M is obtained.



Ref. 3

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－59354
（P2000－59354A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	５Ｋ０１３
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ｅ	
			６３０Ｄ	
	６４０		６４０Ｂ	
	６６０		６６０Ａ	

審査請求　未請求　請求項の数４　ＯＬ　（全５頁）　最終頁に続く

(21)出願番号　特願平10－224433

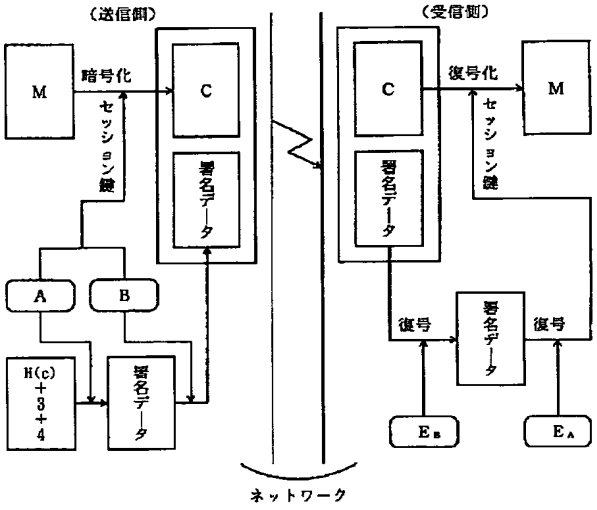
(22)出願日　平成10年８月７日(1998.8.7)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　矢野義博
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内
(72)発明者　林　昌弘
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内
(74)代理人　100092495
弁理士　蛭川　昌信　（外７名）

最終頁に続く

(54)【発明の名称】　可搬記録媒体を利用したセッション鍵の生成方法およびデータ配送システム

(57)【要約】
【課題】　セッション鍵も公開鍵もネットワーク上に流さず、鍵情報が解読される危険性を回避する。
【解決手段】　指標が付された複数の鍵情報を有する同一の鍵テーブルと、相手方の公開鍵がそれぞれ格納された可搬記録媒体を送信側および受信側に配置し、任意に指定された指標に対応する鍵情報をセッション鍵とし、前記任意に指定された指標を可搬記録媒体に格納されている秘密鍵でデジタル署名してセッション鍵情報として送信するようにしたものである。



1

【特許請求の範囲】

【請求項１】　指標が付された複数の鍵情報を有する同一の鍵テーブルと、相手方の公開鍵がそれぞれ格納された可搬記録媒体を送信側および受信側に配置し、任意に指定された指標に対応する鍵情報をセッション鍵とし、前記任意に指定された指標を可搬記録媒体に格納されている秘密鍵でデジタル署名してセッション鍵情報として送信することを特徴とする可搬記録媒体を利用したセッション鍵の生成方法。

【請求項２】　前記可搬記録媒体は送信側および受信側にそれぞれ対応させて複数配置し、複数の可搬記録媒体の各鍵テーブルごとに任意に指定された指標に対応する鍵情報の断片の組み合わせをセッション鍵とし、各鍵テーブルごとに任意に指定された指標の組み合わせ情報を各可搬記録媒体に格納されている秘密鍵でそれぞれデジタル署名してセッション鍵情報として送信することを特徴とする請求項１記載の可搬記録媒体を利用したセッション鍵の生成方法。

【請求項３】　請求項１記載の方法で生成したセッション鍵により送信情報を暗号化し、前記送信情報および前記任意に指定された指標を可搬記録媒体に格納された秘密鍵でデジタル署名した署名データと共にネットワーク上に送信し、受信側では前記署名データを可搬記録媒体に格納されている相手方の公開鍵で復号し、復号により得られた任意に指定された指標の情報から可搬記録媒体に格納された鍵テーブルよりセッション鍵を取得し、取得したセッション鍵により暗号化された送信情報を復号することを特徴とするデータ配送システム。

【請求項４】　請求項２記載の方法で生成したセッション鍵で送信情報を暗号化し、前記送信情報および前記指標の組み合わせ情報を可搬記録媒体に格納されている各秘密鍵でそれぞれデジタル署名した署名データと共に、ネットワーク上に送信し、受信側では前記署名データを可搬記録媒体にそれぞれ格納されている相手方の公開鍵で復号し、復号により得られた指標の組み合わせ情報から可搬記録媒体にそれぞれ格納されている鍵テーブルを利用して鍵情報の断片の組み合わせからなるセッション鍵を取得し、取得したセッション鍵により暗号化された送信情報を復号することを特徴とするデータ配送システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワークを利用してデータを授受する際のセッション鍵の生成方法及びデータ配送システムに関するものである。

【０００２】

【従来の技術】電子メール等の情報をネットワークを介してやり取りする際に起こりうる悪意を有する者からの改ざん、盗聴を防ぐ暗号方式の例を図９により説明する。ここでは、セッション鍵配送に公開鍵暗号方式を用

2

いるものとし、そのため暗号鍵を２つ作成して一方を秘密鍵として自身が秘密の場所に置き、もう１つの鍵を公開鍵として相手に渡し、秘密鍵で暗号化された情報は対応する公開鍵でのみ復号され、公開鍵で暗号化された情報は対応する秘密鍵でのみ復号される。図９において、送信側ではデータの暗号化に使う鍵、すなわちセッション鍵をランダムに生成し、このセッション鍵を用いて送信メッセージＭを暗号化して暗号化された送信メッセージＣを作成する。これと同時に受信者の公開鍵を用いてセッション鍵を暗号化し、暗号化された送信メッセージＣと、暗号化されたセッション鍵とをネットワーク上に送信する。受信側では受信者自身の秘密鍵で暗号化されたセッション鍵を復号してセッション鍵を取得し、取得したセッション鍵で暗号化された送信メッセージＣを復号することにより、元の送信メッセージＭを取得する。

【０００３】

【発明が解決しようとする課題】図９の例では送信側と受信側とで共通に使用するセッション鍵情報がネットワーク上に流れるため、暗号化しているとはいえ鍵情報を解読される危険性があった。本発明は上記課題を解決するためのもので、セッション鍵も公開鍵もネットワーク上に流さず、鍵情報が解読される危険性を回避できるようにすることを目的とする。

【０００４】

【課題を解決するための手段】本発明の可搬記録媒体を利用したセッション鍵の生成方法は、指標が付された複数の鍵情報を有する同一の鍵テーブルと、相手方の公開鍵がそれぞれ格納された可搬記録媒体を送信側および受信側に配置し、任意に指定された指標に対応する鍵情報をセッション鍵とし、前記任意に指定された指標を可搬記録媒体に格納されている秘密鍵でデジタル署名してセッション鍵情報として送信することを特徴とする。また、本発明は、前記可搬記録媒体は送信側および受信側にそれぞれ対応させて複数配置し、複数の可搬記録媒体の各鍵テーブルごとに任意に指定された指標に対応する鍵情報の断片の組み合わせをセッション鍵とし、各鍵テーブルごとに任意に指定された指標の組み合わせ情報を各可搬記録媒体に格納されている秘密鍵でそれぞれデジタル署名してセッション鍵情報として送信することを特徴とする。

【０００５】また、本発明のデータ配送システムは、上記の方法で生成したセッション鍵により送信情報を暗号化し、前記送信情報および前記任意に指定された指標を可搬記録媒体に格納された秘密鍵でデジタル署名した署名データと共にネットワーク上に送信し、受信側では前記署名データを可搬記録媒体に格納されている相手方の公開鍵で復号し、復号により得られた任意に指定された指標の情報から可搬記録媒体に格納された鍵テーブルよりセッション鍵を取得し、取得したセッション鍵により暗号化された送信情報を復号することを特徴とする。ま

た、本発明は、上記の方法で生成したセッション鍵で送信情報を暗号化し、前記送信情報および前記指標の組み合わせ情報を可搬記録媒体に格納されている各秘密鍵でそれぞれデジタル署名した署名データと共に、ネットワーク上に送信し、受信側では前記署名データを可搬記録媒体にそれぞれ格納されている相手方の公開鍵で復号し、復号により得られた指標の組み合わせ情報から可搬記録媒体にそれぞれ格納されている鍵テーブルを利用して鍵情報の断片の組み合わせからなるセッション鍵を取得し、取得したセッション鍵により暗号化された送信情報を復号することを特徴とする。

【０００６】

【発明の実施の形態】以下、本発明の実施例の形態について説明する。図１は本発明の可搬記録媒体と端末装置を用いたシステム概念図、図２は可搬記録媒体の構成を説明する図、図３は送信側と受信側に配される可搬記録媒体内の鍵情報を説明する図、図４は本発明のセッション鍵生成のための鍵テーブルを説明する図、図５はセッション鍵による暗号化および復号を説明する図、図６は可搬記録媒体を利用したデータ配送システムを説明する図、図７は送信側処理を説明する図、図８は受信側処理手順を説明する図である。

【０００７】図１において、端末装置１に対してＩＣカード等の可搬記録媒体２をセットし、ＰＩＮ（パーソナル・アイデンティフィケイション・ナンバー）を確認すると、端末装置１からは可搬記録媒体２に対して、コマンド（命令）を送信し、これを受信した可搬記録媒体２はコマンドを解釈して書き込み、読み取り、読み出し等の処理を実行し、処理結果をレスポンスとして端末装置１に返すようになっている。本発明では、可搬記録媒体、あるいは端末装置１が乱数発生機能を有している。

【０００８】図２に示すように、可搬記録媒体２はＣＰＵ２０、ＲＡＭ２１、ＲＯＭ２２、ＥＥＰＲＯＭ２３を有しており、ＲＯＭ２２に記憶されているプログラムをＣＰＵ２０に読み込み、端末装置１から送信されるコマンドをＩ／Ｏポートを通して受信すると、コマンドと共に送信されたデータを読み込んで、必要な処理を行い、結果をＥＥＰＲＯＭ２３の所定のファイルエリアに書き込み、Ｉ／Ｏポートを通してレスポンスを出力する。

【０００９】ここで説明する例は、図３に示すように、送信側、受信側にそれぞれ互いに相手方の公開鍵を格納した対応する２枚づつの可搬記録媒体を配置する。送信側の可搬記録媒体Ａと受信側の可搬記録媒体Ｘ、送信側の可搬記録媒体Ｂと受信側の可搬記録媒体Ｙがそれぞれ対応し、可搬記録媒体Ａには自身の秘密鍵D_Aと可搬記録媒体Ｘの公開鍵E_Xが格納され、可搬記録媒体Ｘには自身の秘密鍵D_X、可搬記録媒体Ａの公開鍵E_Aが格納されている。同様に、可搬記録媒体Ｂには自身の秘密鍵D_Bと可搬記録媒体Ｙの公開鍵E_Yが格納去れ、受信側の可搬記録媒体Ｙには自身の秘密鍵D_Yと可搬記録媒体Ｂの公開鍵E_Bが格納されている。このように、予め相手の公開鍵を可搬記録媒体に格納してこれを配付するため、公開鍵がネットワーク上に流れるようなことはなく、第３者あるいは自身においてさえも内容を知ることができない。

【００１０】図４は送信情報を暗号化し、また復号するためのセッション鍵を生成するための鍵テーブルである。可搬記録媒体内、あるいは可搬記録媒体のデータを読み込んで処理する端末装置内には、図４（ａ）、（ｂ）に示すような鍵テーブルが格納されている。鍵テーブルは、暗号鍵を生成するための暗号鍵データと、これに対応する指標からなっている。可搬記録媒体Ａには、指標１、２、……ｎに対応して、例えば、８バイトの暗号鍵情報

a_{11} a_{12} …… a_{18}
a_{21} a_{22} …… a_{28}
・
・
a_{n1} a_{n2} …… a_{n8}

が格納される。また、可搬記録媒体Ｂには、指標１、２、……ｎに対応して、８バイトの暗号鍵情報

b_{11} b_{12} …… b_{18}
b_{21} b_{22} …… b_{28}
・
・
・
b_{n1} b_{n2} …… b_{n8}

が格納される。このような鍵テーブルを格納した可搬記録媒体の指標１、２……ｎのうちのいずれかの値をランダムに発生させる。この発生は、可搬記録媒体自身でも端末装置でもどちらで行うようにしてもよい。１、２……ｎをランダムに発生させた結果、可搬記録媒体Ａでは「３」、可搬記録媒体Ｂでは「４」となったとすると、可搬記録媒体Ａの指標「３」に対応する暗号鍵データの先頭４バイト、可搬記録媒体Ｂの指標「４」に対応する暗号鍵データの指標４バイトを組み合わせた

a_{31} a_{32} a_{33} a_{34} b_{45} b_{46} b_{47} b_{48}

がセッション鍵となるようにしておく。

【００１１】図５（ａ）に示すように、送信情報Ｍは前記指標の組み合わせに対応して生成したセッション鍵「a_{31} a_{32} a_{33} a_{34} b_{45} b_{46} b_{47} b_{48}」を用いて暗号化され、暗号文Ｃが得られる。また、図５（ｂ）に示すように、このセッション鍵を利用してＣからＭへ復号される。

【００１２】このようなセッション鍵鍵生成方法を用いてデータを暗号化して送信し、復号する場合を図６により説明する。上記したように、可搬記録媒体Ａ、可搬記録媒体Ｂからランダムに発生させた指標の組み合わせによりセッション鍵が得られ、これにより送信情報Ｍが暗号化されて、暗号文Ｃが得られる。一方、暗号文Ｃの情

報をハッシュ処理したハッシュ値Ｈ（ｃ）と、前記ランダムに発生させた指標「３」、「４」の組み合わせ情報を可搬記録媒体Ａの秘密鍵D_Aでデジタル署名し、さらにこの署名データに対して可搬記録媒体Ｂの秘密鍵D_Bでデジタル署名し、この署名データを暗号文Ｃと共に、ネットワーク上に送信する。受信側では相手の公開鍵を持っているので、署名データを可搬記録媒体Ａ、可搬記録媒体Ｂの公開鍵E_A、E_Bで復号すると、前記テーブルの指標「３」、「４」が得られる。受信側の可搬記録媒体にも同じ鍵テーブルが格納されているので、指標「３」、「４」が分かると、鍵テーブルからセッション鍵「a_{31} a_{32} a_{33} a_{34} b_{45} b_{46} b_{47} b_{48}」が得られる。このセッション鍵により暗号文Ｃを復号することにより、送信情報Ｍが得られることになる。

【００１３】図８により送信側の処理を説明すると、まず、鍵テーブルの指標をランダムに発生させ（Ｓ１）、発生させた指標を組み合わせてセッション鍵を生成する（Ｓ２）。生成したセッション鍵で送信情報を暗号化し（Ｓ３）、送信情報をハッシュ処理する（Ｓ４）。次いで、ハッシュ値と指標の組み合わせに対して送信者の秘密鍵でデジタル署名して、送信者が真正であることを担保し（Ｓ５）、暗号文と署名データをネットワーク上に送信する。

【００１４】図９により受信側の処理を説明すると、署名データを送信者の公開鍵で復号し（Ｓ１１）、指標の組み合わせを取得する（Ｓ１２）。次いで、受信側でもっている鍵テーブルにより、セッション鍵を取得し（Ｓ１３）、これを用いて暗号文を復号する（Ｓ１４）。なお、図９には省略したが、Ｓ１２で得られたハッシュ値と受信側で暗号文から計算したハッシュ値とを照合することにより、ネットワーク伝送途中での通信文に対する改ざんの有無を確認することができる。

【００１５】なお、上記例においては、送信側、受信側ともに可搬記録媒体を２枚づつ用意し、それぞれ対応する公開鍵を持つようにしたが、それぞれ１枚づつ可搬記録媒体を用意し、同様に対応する公開鍵と、同じ鍵テーブルを持つようにしても同様にネットワーク上にセッション鍵、公開鍵を流さずに情報を送信することができる。また、可搬記録媒体が２枚づつでなく、３枚以上ずつ配し、それぞれのカードに対応した鍵テーブルを持ちあわせ各テーブルの指標をランダムに発生させて組み合わせによりセッション鍵を生成するようにしても良い。

【００１６】

【発明の効果】以上のように本発明によれば、送信側、受信側に互いに相手の公開鍵とセッション鍵を生成するための鍵テーブルをそれぞれ格納しておき、ネットワーク上にはセッション鍵を生成するための指標の組み合わせデータのみ流れ、さらに公開鍵は一切流さず可搬記録媒体に格納されているので、第３者の目にふれることがなく、さらに送信者、受信者自身もその鍵を知ることができないので、鍵が解読される危険性を回避することができる。また、公開・秘密鍵を管理運用するコストの低減が可能である。

【図面の簡単な説明】

【図１】　可搬記録媒体と端末のシステム概念図図である。

【図２】　可搬記録媒体の構成を説明する図である。

【図３】　可搬記録媒体内の鍵情報を説明する図である。

【図４】　本発明の鍵テーブルを説明する図である。

【図５】　セッション鍵による暗号化および復号を説明する図である。

【図６】　本発明のデータ配送システムを説明する図である。

【図７】　送信側処理を説明する図である。

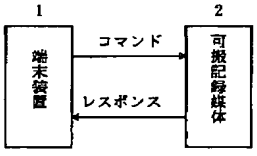
【図８】　受信側処理手順を説明する図である。

【図９】　従来の盗聴を防ぐ暗号方式の例を説明する図である。

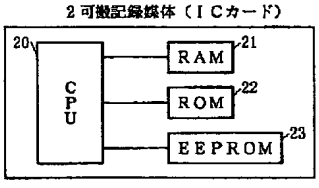
【符号の説明】

１…端末装置、２…可搬記録媒体、Ｍ…送信情報、Ｃ…暗号文。

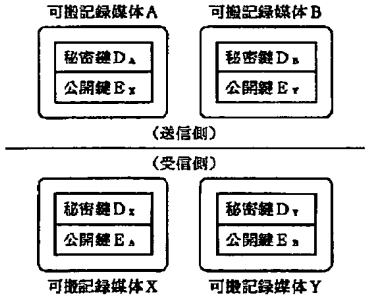
【図１】



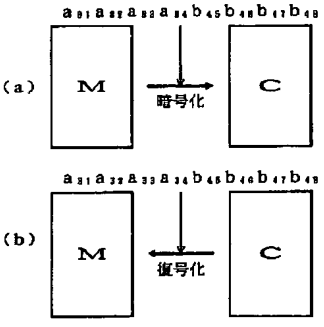
【図２】



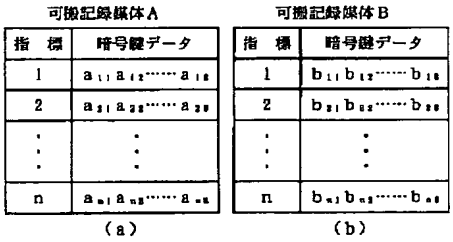
【図３】



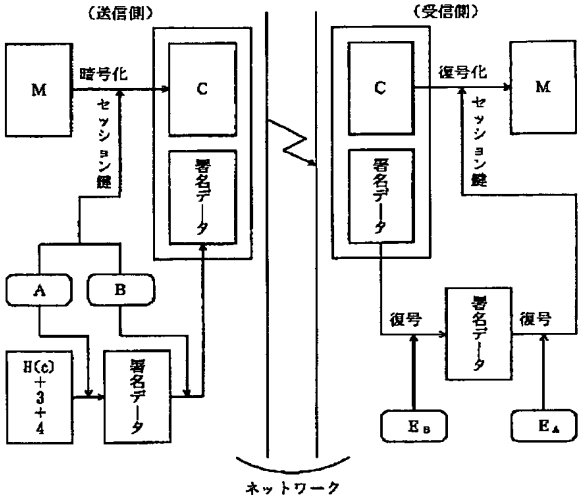
【図５】



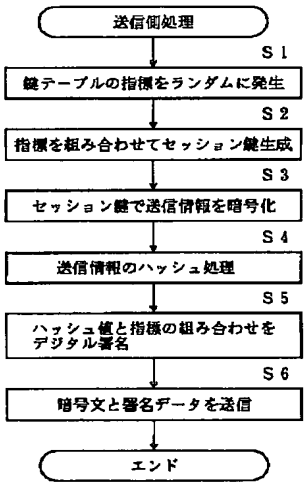
【図４】



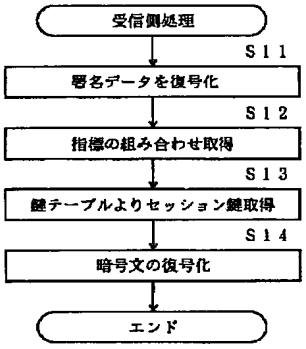
【図６】



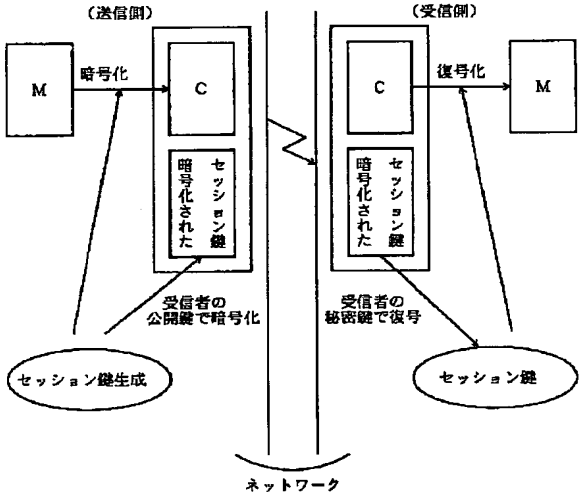
【図７】



【図８】



【図９】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
H04L 9/08		H04L 9/00	601D 601E

(72)発明者　半田富己男
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

(72)発明者　平野晋健
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

Fターム(参考)　5K013 AA03 EA02 FA03 GA08 HA04 JA05